COMPUTER & INFORMATION TECHNOLOGY CENTER

Information Classification Policy

Document Controls

This document is reviewed every six months

Document Reference	PAAET-PLCY-Information Classification
Document Title	Information Classification Policy
Document Owner	Abdullah Aldousari
ISO 27001:2013 reference	A.8.2 Information Classification
Security Classification	Internal - Restricted
Stored	http://sp13.paaet.edu/sites/TecDep
Next Review Date	14th Aug, 2017
Document Status	Final

Document Review and Approval History

Date	Version	Amended by	Reviewer / Approver	Remarks	RFC#
18th April, 2016	Draft v1.0	Reena Varghese			
21st April 2016	Draft v1.1	Reena Varghese	Jessy Sakariah	Reviewer	
14th Feb, 2017	Draft v1.3	Abdullah AlDousari	**Rabie Al-Mejbas**		

Document Distribution List

Sl.No.	Name and Department	Purpose
1	ISO team : • Rabie Al-Mejbas • Rajiv Prakash • Nadia AL Saleh • Shaikha AL Barak • Mai AlAbdulqader • Abdullah Aldousari	Start implementing this policy on all documentations.
2	All CIC	To comply with the policy

CONTENTS

CONFIDENTIALITY STATEMENT

This document includes confidential information related to the Computer and Information Technology Center (**CIC**) at the Public Authority for Applied Education and Training (**PAAET**), shall not be distributed to any persons other than those mentioned in the distribution list herein, and shall be used solely for **CIC**'s internal purpose.

1.0 INTRODUCTION

Information Classification, Labelling & Handling process deals with the proper classification, labelling and handling of all Information owned or under the custody of CIC at **PAAET**.

2.0 OBJECTIVE

The objective of the Information Classification, Labelling & Handling is to ensure that critical assets receive an adequate level of protection, are labelled and handled appropriately. These standards ensure the baseline of the implementation of guidelines.

3.0 SCOPE

These standards apply to all PAAET's Information owners, PAAET's Services team and covers the following assets:

- Physical assets: computer equipment, communication equipment, security equipment, magnetic media, other technical equipment;
- Software assets: application software, development tools and utilities;
- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, archived information.

4.0 POLICY

4.1 Physical and Software Classification

The following provides a summary of the Information classification levels that have been adopted by PAAET and are designed to cover the physical and software assets.

Critical	
Definition	This classification applies to the most sensitive hardware and software which is intended strictly for use within PAAET. It should be always available, secured, and monitored with full access control, date integrity too is very important here.
Examples	Data Centre Servers, Core Switches, Data Centre Firewalls, Data Centre Components.

Important	
Definition	This classification applies to less sensitive hardware and software which is intended for use within PAAET. Like critical, important should always be secured, monitored with full access control. Confidentiality should appear on this category as these systems must be controlled by one user unlike critical.
Examples	Manager PC's, Admin PC's, and Important Printers.

Non-Critical	
Definition	This classification applies to all other information which does not clearly fit into any of the other two classifications i.e. Critical and Important. Here only system security and access control is our main priority.
Examples	Employee PC's, Lab PC's, and Shared Printers

4.2 Information Classification

The following provides a summary of the Information classification levels that have been adopted by PAAET and are designed to cover the information assets.

Confidential	
Definition	This classification applies to the most sensitive business information which is intended strictly for use within PAAET. Its unauthorized disclosure could seriously and adversely impact PAAET, its share-holders, its business partners, and/or its customer/students leading to legal and financial repercussions and adverse public opinion.
Examples	Trade secrets, student data, Payroll information, financial reports, contracts and agreements with partners.

Internal – Restricted	
Definition	This classification applies to less sensitive business information which is intended for use within PAAET. Its unauthorized disclosure could adversely impact PAAET, its employees, and/or its customers but the impact would not be devastating. Information, which is considered to be private to the organization, is included in this classification.
Examples	Employee performance evaluations, Proposals, Contracts, analyses of competitive products / services, internal audit reports and intellectual capital of PAAET which comprises the collective experience, skill, knowledge and information of PAAET and its people.

Internal – Unrestricted	
Definition	This classification applies to all other information which does not clearly fit into any of the other two classifications i.e. Confidential or Internal Restricted. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact PAAET, its employees, its shareholders, its business partners, and/or its customers.
Examples	Training materials, and policy manuals.

Public	
Definition	This classification applies to information which has been explicitly approved by PAAET management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.
Examples	Student Results, Service brochures, advertisements, job opening announcements, and press releases.

4.3 Information Labelling

Labeling ensures that Information is handled appropriately. Where no labeling exists the Information shall be treated as Public.

- **Confidential:** Confidential Information shall be labeled “Confidential under (mandate e.g.: ISO 27001)” indicating that the Information falls into a regulatory mandate.
- **Internal - Restricted**: Confidential Information shall be labelled as Internal Restricted:

(e.g.: salary information, HR information, Privileged & Confidential (e.g.: legal advice and relate material, etc.)

- **Internal - Unrestricted:** There is no need to place a label on Information that is spread internally within the organization.
- **Public:** Public Information does not require labeling.

4.4 Information Handling

4.4.1 Handling of "Confidential" or "Internal - Restricted" Information

PAAET shall not remove or forward "Confidential" or "Internal - Restricted" information from its premises unless prior approval from the Data Owners has been obtained. This standard includes portable computers with hard disks, CDs, USB, floppy disks, hardcopy outputs, paper memos and the likes. An exception is made for authorized off-site backups. An audit trail must log all attempts (successful or unsuccessful) to access "Confidential" information.

4.4.2 Storage and Transmission of "Confidential" or "Internal - Restricted" Information

PAAET shall ensure that the storage media is physically secured. Storage and transmission of "Confidential" or "Internal - Restricted" information at rest or over communications networks shall be encrypted. Wherever possible, PAAET shall implement encryption and password control over the storage or media containing "Confidential" or "Internal - Restricted" information in accordance with the requirement stipulated in Information Security policy.

4.4.3 Re-classification of Information

PAAET's Data Owners are required to re-classify the classification of information when warranted within a reasonable time. Based on the classification criteria mentioned in Section 4.1 "Information Classification", the information can be re-classified to a different level. For example, financial data before it is released may be classified as "Confidential" or "Internal-Restricted". Once the data is made public, such as published in journals, examinations, and quarterly or annual reports, it should be re-classified as "Public".

4.4.4 Release of Information to Third Parties

PAAET shall ensure that all "Confidential", "Internal - Restricted" or "Internal - Unrestricted" information is protected from disclosure to third parties by default. Exceptions are permissible if the release of this information is clearly needed to accomplish a certain objective of PAAET based on

the principles of purpose, reasonableness and non-excessiveness, and if the identity of the receiving party has first been confirmed. The Data Owner needs to establish requirements for any disclosures of “Confidential”, “Internal Restricted” or “Internal Unrestricted” information to third parties and any disclosures of such information to third parties must be subject to a written agreement specifying what information is restricted and how this information may and may not be used. Consent from the Data Owners must be sought prior to the release of “Confidential” or “Internal - Restricted” information to third parties.

4.4.5 Retention and Disposal of Information

Every PAAET IT member has the responsibilities to consider security when using and disposing of information in all circumstances. Departments or contractors that are regarded as key data owners, controllers or custodians shall be responsible for defining and documenting the retention period of critical data. The legal requirements and responsible parties should also be specified.

PAAET shall define appropriate retention periods for certain kinds of information. Every department or contractor should establish procedures appropriate to the information held and processed by them, and ensure that all relevant parties are aware of those procedures.

Departments or contractors must retain records and information if:

- They are likely to be needed in the future, unless a specific retention cycle has already mandated by specific policy to ensure their availability timely, such as the existing policy on email retention.
- Regulation or statute requires their retention, or;
- They are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts or to allow PAAET to respond to discovery requests, subpoenas, investigatory demands and other requests for information related to legal or regulatory proceedings.

Sensitive information should be disposed of according to the respective disposal procedures for different classifications of information in order to ensure complete removal of “Confidential” “Internal - Restricted “or “Internal - Unrestricted” information, including both paper based and electronic forms. Disposal procedures include shredding, low level formatting, degaussing of hard disk drives etc. Unauthorized destruction or disposal of PAAET’s sensitive information will subject the perpetrator to disciplinary action including termination and prosecution.

4.4.6 Backup and Recovery

PAAET must implement the same level of security measures for the backup of “Confidential” “Internal - Restricted “and “Internal - Unrestricted” information.

Backup procedures shall be documented and in accordance with the security requirement for handling of “Confidential”, “Internal - Restricted “and “Internal Unrestricted” information. In particular, the following details shall be specified:

- Backup Scope (i.e. category and classification of information to be backed up);
- Backup Frequency;
- Backup Media;
- On-site and/or Off-site Backup Location;
- Backup Retention;
- Logical and Physical Security Measures for Backup Media and Location; and
- Backup Method (i.e. Incremental, Differential or Full).

Request to restore “Confidential”, “Internal - Restricted “and “Internal - Unrestricted” information from backup media must be approved by Management and respective Data Owners. PAAET must restrict the access to the restored data to authorized members.

Backup and recovery of “Confidential”, “Internal - Restricted “and “Internal - Unrestricted” information must be performed by authorized IT Operations staff and audited by independent parties at least annually.

5.0 REFERENCES

1) ISO/IEC 27001:2013 - [A.8.2] – Information Classification

6.0 ASSOCIATED DOCUMENTS

1) Information Security Policy